In the Claims

1. (Currently Amended) A printer device comprising:

a data input device for receiving an encrypted digital document file;

a decryption algorithm for decrypting said received document file;

a controller for controlling printing of an image of data contained in said received document file, wherein said controller operates to read quantity permission data from said document file, said quantity permission data specifying a number of copies of said document file authorized to be printed, and wherein said controller operates to generate a confirmation message confirming receipt of said document file; and

a printer mechanism for printing a physical copy of said document file,

wherein said controller operates to control printing of the number of copies authorized to be printed, and after printing the number of copies authorized to be printed of the document file, automatically deletes said document file from said memory.

2. (Original) The printer device as claimed in claim 1, further comprising a decryption key locally stored in said printer device.

3. (Original) The printer device as claimed in claim 1, comprising a network interface for receiving said encrypted digital document file over a network.

4. (Original) The printer device as claimed in claim 1, wherein said controller stores a unique device identification data uniquely identifying said printer device, said controller operating to:

compare a received unique identifier data contained in said received document file with said stored unique device identifier; and

if said received unique device identifier data differs from said stored unique device identifier data, delete said document file.

5. (Original) The printer device as claimed in claim 1, wherein said controller stores a unique device identification data uniquely identifying said printer device, said controller operating to:

compare a received unique identifier data contained in said received document file with said stored unique device identifier; and

if said received document identification data is identical to said received unique device identifier data, control said print mechanism to print at least one said physical copy of said document file.

6. (Cancel)

7. (Cancel)

8. (Currently Amended) The printer device as claimed in claim 1, wherein ~~wherein;~~

~~said controller operates to generate a confirmation message confirming receipt of said document file;~~

said confirmation message comprises a time and date data, specifying a time and date of receipt of said document file and a number of copies printed data, specifying a number of copies of said document file physically printed by said print mechanism.

9. (Currently Amended) A printer device comprising:

a data input device for receiving an encrypted digital document file;

a decryption algorithm for decrypting said received document file;

a controller for controlling printing of an image of data contained in said received document file, wherein said controller operates to read a quantity permission data content from said document file, said quantity permission data specifying a number of authorized copies of said document file to be printed, and wherein said controller operates to generate a confirmation message confirming receipt of said document file; and

a printer mechanism for printing a physical copy of said document file, wherein said controller operates to check a unique device identification data contained in said document file with a stored unique device identification data of said printer device, and provided a successful match is found, to print said physical copy of said document file and to delete said document file after printing said physical copy; and

if said received unique device identifier differs from said stored unique device identifier data, said controller operates to delete said document file without printing a physical copy of said document file.

10. (Currently Amended) A computer system configured for sending secure encrypted document files, said system comprising:

a data processor;

a memory;

an encryption algorithm capable of encrypting a document file;

a device selector for selecting a said uniquely identifiable recipient device;

a file selector for selecting a document file;

a stored list of a set of authorized recipient devices, each said recipient device identified by a unique device identifier data inaccessibly embedded within said computer ~~entity~~system;

wherein said computer ~~entity~~ system operates to:

select at least one document file, wherein the selected document file comprises quantity permission data specifying a number of copies of said document file authorized to be printed;

select at least one said uniquely identifiable recipient device to send said document to:

encrypt said document files; and

address said at least one document file to said selected uniquely identified recipient device; and

at least one recipient printer device, said recipient printer device capable of receiving an encrypted document file, establishing that said encrypted document file is intended for said recipient printer device, generate a confirmation message confirming receipt of said document file, decrypting and printing said encrypted document file, and automatically deleting said document file after printing a physical copy of a document from said document file.

11. (Previously Presented) The system as claimed in claim 10, further comprising:

a network interface capable of sending said document file over a network to said selected recipient device.

12. (Currently Amended) The system as claimed in claim 10, wherein:

said controller operates to read a quantity permission data content of said document file, said quantity permission data specifying a number of authorized copies of said document file to be printed~~; and~~

~~said controller controls said printer mechanism such that said permitted quantity of physical copies of said document file are printed~~.

13. (Currently Amended) The computer system as claimed in claim 10, ~~wherein said~~additionally comprising a user interface ~~further displays~~configured to display:

data describing an encryption method used for sending said document.

14. (Currently Amended) The computer system as claimed in claim 10, ~~wherein said~~additionally comprising a user interface ~~displays~~configured to display:

an acknowledgement message data describing receipt of said document file by [[a]] said recipient device.

15. (Previously Presented) A distributed secure document printing system, said system comprising:

at least one sending computer entity, capable of sending an encrypted electronic document file, said document file having an encrypted data content, and a unique device identifier data identifying a recipient printer device to which said document file is intended to be printed by; and

at least one recipient printer device, said recipient printer device capable of receiving said encrypted document file, establishing that said document file is intended for said recipient printer device, decrypting and printing said document file, and automatically deleting said electronic document file after printing a physical copy of a document from said document file;

wherein said recipient printer device is configured to send a confirmation message back to said sending computer entity, confirming receipt of said document file, and confirming printing of a specified permitted number of copies of said document file, wherein the specified permitted number of copies of said document file is contained within the document file.

16. (Original) The system as claimed in claim 15, wherein said recipient printer device is capable of reading a permitted quantity data content of said document file; and

said recipient printer device operates for printing a number of physical copies of said document file, corresponding to said permitted quantity data.

17. (Cancel)

18. (Previously Presented) A method of securely communicating an electronic document file over a network, said method comprising the steps of:

encrypting said document file;

specifying a recipient device for sending said document file to, said recipient device being uniquely identifiable by a unique device identifier data;

attaching said unique identifier data to said document file;

sending said document file in encrypted format to said intended recipient device;

receiving said transmitted document file and decrypting said document file;

reading said unique device identifier data of said document file;

if said unique device identifier data of said document file corresponds to a unique device identifier data of said recipient device, printing a physical copy of said document file and automatically deleting said document file;

if said unique device identifier data of said document file does not correspond with said unique device identifier data of said recipient device,

deleting said received document file without printing a physical copy of said document file; and

sending, from said recipient device, a confirmation message back to said sending computer entity, confirming receipt of said document file, and confirming printing of a specified permitted number of copies of said document file, wherein the specified permitted number of copies of said document file is contained within the document file.

19. (Cancel)

20. (Cancel).

21. (Previously Presented) A method of secure printing of a received document file, said method comprising the steps of:

receiving said document file in encrypted format at a receiving device;

decrypting said document file;

reading a unique device identifier data identifying a recipient device for which said document file is intended;

comparing said unique device identifier data with a locally stored device identifier data stored at said receiving device;

if said received unique device identifier data corresponds with said locally stored device identifier data, printing at least one physical copy of said document file and automatically deleting said document file;

if said received unique device identifier data differs from said stored unique device identifier data, deleting said document file; and

sending, from said recipient device, a confirmation message back to said sending computer entity, confirming receipt of said document file, and confirming printing of a specified permitted number of copies of said document file, wherein the specified permitted number of copies of said document file is contained within the document file.

22. (Original) The method as claimed in claim 21, further comprising the step of:

deleting said electronic document file, after printing said physical copy of said document file.

23. (Original) The method as claimed in claim 21, further comprising the step of:

reading a permitted quantity data describing a permitted quantity of copies of said document file; and

printing said permitted quantity of copies of said document file.

24. (Original) The method as claimed in claim 21, wherein said document file, after decryption is prevented from being viewed on a visual display device prior to printing.

25. (Original) The method as claimed in claim 21, wherein said document file is received via an intermediary carrier device having data storage capability.

26. (Currently Amended) A method of sending a document file for printing by a specified authorized recipient printing device, said method comprising the steps of:

selecting a content of said document file;

encrypting said content;

attaching a unique device identifier data, identifying a recipient device to which said document file is to be sent;

sending said document file to said recipient device; ~~and~~

adding a permitted quantity data to said document file, said permitted quantity data specifying a permitted number of copies of said document file which can be ~~printed.~~ printed; and

receiving a confirmation message confirming receipt of said document file.

27. (Cancel)

28. (Original) The method as claim in claim 26, further comprising the steps of:

storing a document history data, said document history data specifying for said document file:

a list of at least one recipient device to which said document file may be sent;

a number of permitted copies of said document file which are permitted to be printed by each said recipient device.

29. (Currently Amended) A computer entity comprising a data processor, a data storage device, a printer port, and having an attached printer device, said computer entity comprising:

a module for decrypting an encrypted document file;

a unique device identifier for identifying said computer entity;

wherein said computer entity operates to:

receive a document file in encrypted format;

decrypt said document;

extract a unique device identifier data from said document;

compare said extracted unique identifier data with said unique device identifier of said computer entity;

if a match is found between said received unique device identifier data of said document and said unique identifier of said computer entity, send a said document file for printing by said attached printer device; and

after sending said document to said printer device, delete said document file from said computer entity; ~~and~~

adding a permitted quantity data to said document file, said permitted quantity data specifying a permitted number of copies of said document file which can be ~~printed.~~ printed; and

receiving a confirmation message confirming receipt of said document file.

30. (Currently Amended) A method of secure printing of a received document file, said method comprising the steps of:

receiving said document file in encrypted format;

reading a unique device identifier data identifying a recipient device for which said document file is intended;

comparing said unique device identifier data with a locally stored identifier data corresponding to a local computer entity device;

if said locally stored identifier data differs from said unique device identifier data identifying said recipient device for which said document file is intended, deleting said document file without printing any physical copies of said document file; ~~and~~

printing a number of physical copies of said document file, corresponding to a permitted quantity defined in said document file, wherein the specified permitted number of copies of said document file is contained within the document file and wherein said document file is automatically ~~deleted.~~ deleted; and

sending a confirmation message confirming receipt of said document file.

31. (Currently Amended) A method of secure printing of a received document file, said method comprising the steps of:

receiving said document file in encrypted format;

sending a confirmation message confirming receipt of said document file;

reading a unique device identifier data identifying a recipient device for which said document file is intended;

comparing said unique device identifier data with a locally stored device identifier data;

reading a permitted quantity data describing a permitted quantity of copies from said document file; ~~and~~

if said received unique device identifier data corresponds with said locally stored device identifier data, printing said permitted quantity of copies of said document file and automatically deleting said document file; and

printing a number of physical copies of said document file, corresponding to a permitted quantity defined in said document file.

32. (Currently Amended) A printer device comprising:

a data input device for receiving an encrypted digital document file;

a decryption algorithm for decrypting said received document file;

a controller for controlling printing of an image of data contained in said received document file, for sending a confirmation message upon receipt of the document file and for automatically deleting said document file; and

a printer mechanism for printing a physical copy of said document file,

wherein said printer device locally stores a decryption key for operating said decryption algorithm to decrypt said received document file; ~~and~~

wherein said printer device is configured to send a confirmation message back to said sending computer entity, confirming receipt of said document file, and confirming printing of a specified permitted number of copies of said document file, wherein the specified permitted number of copies of said document file is contained within the document file.

33. (Currently Amended) A printer device comprising:

a data input device for receiving a digital document file;

a controller for controlling printing of an image of data contained in said received document file and for sending a confirmation message upon receipt of the document file; and

a printer mechanism for printing a physical copy of said document file,

wherein said controller operates to compare a received unique identifier data contained in said received document file with a locally stored unique device identifier data stored at said printer device and operates to control printing of a predetermined quantity of said physical copy, wherein said predetermined quantity is specified in said received document file;

if said received unique identifier data matches said stored unique device identifier, control printing of at least one said physical copy of said document file and automatically delete said document file; and

if said received unique identifier data contained the said received document file does not match said stored unique device identifier data, to inhibit printing of any physical copies of said document file.

34. (cancel)

35. (Previously Presented) A printer device comprising:

a data input device for receiving an encrypted digital document file;

a decryption algorithm for decrypting said received document files;

a controller for controlling printing of an image of data contained in said received document file; and

a printer mechanism for printing a physical copy of said document file,

wherein a decryption key is stored locally in said printer device for operating said decryption algorithm to decrypt said received document files;

said controller operates to compare a received unique identifier data contained in said received document file with a locally stored unique device identifier data stored at said printer device;

if said received unique identifier data matches said stored unique device identifier, control printing of at least one said physical copy of said document file and automatically deleting said document file; and

if said received unique identifier data contained the said received document file does not match said stored unique device identifier data, to inhibit decryption of said document file and inhibit printing of any physical copies of said document file;

wherein said printer device is configured to send a confirmation message back to said sending computer entity, confirming receipt of said document file, and confirming printing of a specified permitted number of copies of said document file, wherein the specified permitted number of copies of said document file is contained within said document file.